IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF THE SUBJECT DEVICES CURRENTLY IN THE UNITED STATES DRUG ENFORCEMENT ADMINISTRATION'S POSSESSION AT THE BALTIMORE DISTRICT OFFICE LOCATED IN BALTIMORE, MARYLAND (LISTED ON ATTACHMENT "A")	**Case No.** 19-833-846

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, GLENN HESTER, being duly sworn, depose and state as follows:

INTRODUCTION

1. Your Affiant makes this Affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search warrant authorizing the examination of four cellular telephones and two computers as described in Attachment "A" (collectively referred to as the "SUBJECT DEVICES") which are in the United States Drug Enforcement Administration's possession at the Baltimore District Office in Baltimore, Maryland, and the extraction of electronically stored information identified in Attachment "B" from those devices pursuant to the search protocol set forth in Attachment "C."

2. Investigators found and seized the SUBJECT DEVICES while executing search warrants issued by United States Magistrate Judge J. Mark Coulson on February 13, 2019. (The warrant (No. 19-0585 JMC) and affidavit submitted in support of it are attached as Exhibit 1 and incorporated by reference herein.)

3. Your Affiant submits that probable cause exists to believe that the SUBJECT DEVICES contain evidence of violations of Title 21 U.S.C. § 846 (Conspiracy to Distribute and

Possess with Intent to Distribute Controlled Substances), violations of Title 18 U.S.C. § 3147 (Commission of a Crime while on Release), Maryland Criminal Code § 5-701 (Unauthorized Dispensing of a Prescription Medication), Title 18 U.S.C. § 1513 (Retaliating Against a Witness), and Title 18 U.S.C. § 1958 (Murder for Hire); or the SUBJECT DEVICES were designed for use, intended for use, or used in committing the aforementioned crimes.

IDENTIFICATION OF THE DEVICES

4. As detailed further on Attachment A, the SUBJECT DEVICES—all of which are in the DEA's possession at the Baltimore District Office in Baltimore, Maryland—is as follows:

ITEM	DESCRIPTION	SEIZURE LOCATION
Cellphone No. 1	**Black LG cellphone, IMEI:353934093715384;SN:809VTDN371538 Attachment "D"**	**Seized from the person of David ROBINSON**
Cellphone No. 2	**Black LG cellphone with a cracked screen, IMEI: 354063082587114; SN: 704CQGW258711, Attachment "E"**	**Seized from 2015 Mercedes SUV**
Cellphone No. 3	**Black Apple IPhone, (Model A1784), IMEI: 356565081254643, Attachment "F"**	**Seized from 2015 Mercedes SUV**
Cellphone No. 4	**Apple IPhone 10s (IMEI: 353284077244104 Model A1687, FCC-ID BCG-E2944A), Attachment "G"**	**Seized from Maisha MCCOY**
Computer No. 1	**Red HP laptop computer, SN: CND5250KS8, (Model 15-AF075NR), Attachment "H"**	**4 Coral Berry Court, Baltimore, MD**
Computer No 2	**HP Pavilion computer, SN: MXX61603ZL, (Model 550-1533W), Attachment "I"**	**4 Coral Berry Court, Baltimore, MD**

5. In your Affiant's training and experience, your Affiant knows that the DEA has stored the SUBJECT DEVICES in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the DEA's possession. The applied-for warrants would authorize the forensic

examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

YOUR AFFIANT

6. Your Affiant has been a police officer of the Baltimore Police Department since February 1986. He has been assigned as a Task Force Officer ("TFO") with the DEA's Tactical Diversion Squad in Baltimore, Maryland, since approximately May 2005. In this role, your Affiant investigates criminal violations related to the diversion of pharmaceutical controlled dangerous substances and prescription medications.

7. Your Affiant has participated in numerous investigations of unlawful drug distribution involving the use of undercover officers, confidential informants, and undercover transactions. In addition, he has conducted physical surveillance, telephone toll analysis, and investigative interviews; applied for and executed search warrants; and assisted in the recovery of substantial quantities of narcotics, pharmaceutical controlled substances, proceeds thereof, and related paraphernalia. Moreover, your Affiant has interviewed individuals involved in the controlled dangerous substance ("CDS") trafficking trade, including drug dealers and users as well as confidential informants, and among the topics covered during such interviews are the habits, lifestyles, and terminology in the CDS trafficking trade.

8. Through your Affiant's training, knowledge and experience, he has become familiar with the manner in which CDS traffickers transport, store, "stash," manufacture, and distribute CDS; the methods by which such traffickers collect and conceal the proceeds of their illegal activities; and the manner in which CDS traffickers use cellular telephones and other electronic devices like computers to facilitate illegal activities and hamper law enforcement investigations.

9. The facts set forth in this Affidavit are based upon your Affiant's personal knowledge, review of documents and other evidence related to this investigation, and communications with other individuals who have personal knowledge of the events and circumstances described herein as well as information gained through training and experience. This Affidavit does not contain all of the information known to your Affiant regarding this investigation. Your Affiant has included only the facts that are sufficient to support a probable cause finding for the issuance of the requested warrant and does not purport to include each and every matter of fact observed or known to your Affiant or other law enforcement officers involved in this investigation.

Use of Electronic Devices by CDS Traffickers

10. Based upon your Affiant's training, experience, and participation in other CDS trafficking investigations, he knows that individuals involved in drug trafficking, including those involved in the diversion of pharmaceutical drugs, often do the following:

a. Maintain books, records, and other documents that relate to the manufacture, transportation, possession, and distribution of controlled substances where they have such information readily accessible to them, including their homes, offices, and electronic devices, such as cellular telephones and personal digital assistants ("PDAs").

b. Store the names, addresses, and/or telephone numbers of associates in their drug trafficking activities on cellular telephones.

c. Use cellular telephones to communicate with their customers and/or co-conspirators via voice calls and text messages. Text messages, voice messages, records of incoming and outgoing communications, emails are often stored on electronic devices such as cell phones.

d. Use multiple cellular telephones and electronic devices in an effort to conceal their activities.

e. Keep logs of drug debts owed by customers or to suppliers, commonly referred to as an "owe sheet" or a "tally sheet" on their cellular telephones or other electronic devices.

11. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS")

technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System

to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory

cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. Based on my training, experience, and research, I know that **Cellphone Nos. 1 - 4** have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

13. Based on my training, experience, and research, I know that **Computers Nos. 1 - 2** have capabilities that allow them to store data, create documents, and access the internet using IP addresses. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that **SUBJECT DEVICES** can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe that things that were once stored on **Computer Nos. 1-2** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person

"deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks

permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). On computers, virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the

device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

PROBABLE CAUSE

19. As detailed further in Exhibit 1, David ROBINSON was a pharmacist who was charged with conspiring to distribute oxycodone and alprazolam, in violation of 21 U.S.C. § 846 and several counts of the distribution of those drugs, in violation of 21 U.S.C. § 841. On October 10, 2018, ROBINSON plead guilty to one (1) count of conspiracy to distribute and possess with intent to distribute Oxycodone and Alprazolam, in violation of 21 U.S.C. § 846, and sentencing was scheduled for February 15, 2019.

20. While on release pending sentencing, investigators learned that ROBINSON was continuing to sell prescription medications and made several controlled purchases of clonidine and promethazine from him. They also learned that he had sought to have an individual murdered that he believed cooperated with law enforcement against him and conducted several controlled meetings and calls during which ROBINSON discussed his plans.

21. On February 13, 2019, the Honorable J. Mark Coulson, United States Magistrate Judge, issued search and seizure warrants for the following:

- A cellular telephone utilized by David ROBINSON, believed to be **Cellphone No. 1**.[1]

[1] Although investigators believe that this warrant provides sufficient basis for the search of Cellphone No. 1, a request for a further warrant is included out of an abundance of caution now that investigators have the specific identifiers for the cell phone, as detailed above and on Attachment A.

- ROBINSON's residence located at 4 Coral Berry Court, Baltimore, Maryland 21209.
- ROBINSON's vehicles: a 2015 Mercedes SUV, 2011 BMW, and 1999 BMW.
- The NEW FRANKFORD FAMILY PHARMACY, located at 5422 Sinclair Lane, Baltimore, Maryland 21206.
- BREATHE 4 SURE PHARMACY SOLUTIONS, located at 643 N. Carey Street, Baltimore, Maryland 21217.
- 9522 Axehead Court, Randallstown, Maryland 21133.

22. Judge Coulson also issued a criminal complaint charging ROBINSON with committing a crime while on release, in violation of 18 U.S.C. § 3147, attempting to retaliate against a witness, in violation of 18 U.S.C § 1513, and attempted murder for hire, in violation of 18 U.S.C. § 1958.

23. On February 14, 2019, ROBINSON was arrested and the above warrants were executed. During a search incident to the arrest of ROBINSON, officers recovered from his person **Cellphone No. 1**. A search of ROBINSON's 2015 Mercedes SUV officers located **Cellphone No. 2** and **Cellphone No. 3**. During the search of ROBINSON's residence, officers recovered **Computer No. 1** and **Computer No. 2**. During the search of the BREATHE 4 SURE PHARMACY SOLUTIONS, officers recovered **Cellphone No. 4**, believed to belong to Maisha MCCOY.

24. During the service of the search and seizure warrants, Agents and officers also recovered an ~~undetermined~~ $3,839.00 GOT amount of cash, one firearm, Oxycodone, Hydrocodone, Xanax, sealed pharmacy stock bottles of Clonidine, various prescription medications, RX receipts, documents, ordering invoices, miscellaneous papers and other items of evidentiary value.

25. Investigators had found that recent order of drugs for the New Frankford Family Pharmacy had been placed online. Investigators know that someone would have needed to use a computer or other electronic device to place those online orders. Based on the search of

ROBINSON's residence, where **Computer No. 1** and **Computer No. 2** were found, it appeared that ROBINSON had been attempting to operate the New Frankford Family Pharmacy from his home. Specifically, investigators found written prescriptions, pharmacy labels with various patient's names, invoice stickers, U.S. Official ordering forms, DEA-222, pharmacy records and labels, a fax machine, **Computer No. 2**, and stock pharmacy bottles containing Tramadol, Alprazolam, Oxycodone, and Hydrocodone.

26. Investigators also know that, during controlled calls and meetings with ROBINSON he regularly used a cellular phone to communicate with the confidential source and others. Specifically, the CS indicated that he/she regularly communicated with ROBINSON via cell phone, both via text message and voice calls. The calls the CS placed to ROBINSON in the presence of law enforcement were to a number that came back to an AT&T proprietary phone listed to a Prepaid Customer, with a billing address of 1730 Preston Road, Dallas, TX 75252. A review of toll records for that phone also reflect that ROBINSON has continued to be in contact with several individuals who had previously filled prescriptions at the Frankford Family Pharmacy.

27. ROBINSON's Mercedes SUV (where **Cellphone No. 2** and **Cellphone No. 3** were found) was also used by ROBINSON on several occasions during controlled meetings with the confidential source between December 13, 2018 and February 14, 2019. As a result, investigators believe that these cellphones belong to ROBINSON and were used to facilitate the illegal distribution of prescription medications.

28. Investigators also know that ROBINSON regularly communicated with MCCOY via telephone. A review of toll records show that ROBINSON's cell phone had approximately 289 contacts with a phone registered to Breathe 4 Sure Pharmacy Solutions from May 1, 2018 to February 12, 2019.

29. As a result, investigators believe there is probable cause to believe that **Cellphone Nos. 1-4** will contain the items listed on Attachment B.

CONCLUSION

29. Based upon the information set forth in this Affidavit, your Affiant submits that probable cause exists to believe that the SUBJECT DEVICES (listed in Attachment A) contain evidence of violations of Title 21 U.S.C. § 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances), violations of Title 18 U.S.C. § 3147 (Commission of a Crime while on Release), Maryland Criminal Code § 5-701 (Unauthorized Dispensing of a Prescription Medication), Title 18 U.S.C. § 1513 (Retaliating Against a Witness), and Title 18 U.S.C. § 1958 (Murder for Hire); specifically, the items listed on Attachment B and request a warrant to search those devices using the Search Protocol in Attachment C.

Glenn Hester
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me this 20 day of March, 2019.

Stephanie A. Gallagher
United States Magistrate Judge

ATTACHMENT "A"

The SUBJECT DEVICES are:

ITEM	DESCRIPTION	SEIZURE LOCATION
Cellphone No. 1	**Black LG cellphone, IMEI:353934093715384;SN:809VTDN371538, Attachment "D"**	**Seized from the person of David ROBINSON**
Cellphone No. 2	**Black LG cellphone with a cracked screen, IMEI: 354063082587114; SN: 704CQGW258711, Attachment "E"**	**Seized from 2015 Mercedes SUV**
Cellphone No. 3	**Black Apple IPhone, (Model A1784), IMEI: 356565081254643, Attachment "F"**	**Seized from 2015 Mercedes SUV**
Cell Phone No. 4	**Apple IPhone 10s (IMEI: 353284077244104 Model A1687, FCC-ID BCG-E2944A), Attachment "G"**	**Seized from Maisha MCCOY**
Computer No. 1	**Red HP laptop computer, SN: CND5250KS8, (Model 15-AF075NR), Attachment "H"**	**Seized from 4 Coral Berry Court, Baltimore, MD**
Computer No 2	**HP Pavilion computer, SN: MXX61603ZL, (Model 550-1533W), Attachment "I"**	**Seized from 4 Coral Berry Court, Baltimore, MD**

All of the aforementioned electronic devices are in the possession of the United States Drug Enforcement Administration at its Baltimore District Office located at 200 St. Paul Place, Suite 2222, Baltimore, Maryland 21202.

ATTACHMENT "B"

This warrant authorizes the search and seizure of all records contained within the electronic devices described in Attachment A that relate to violations of Title 21 U.S.C. § 846 (Conspiracy to Distribute and Possess with Intent to Distribute Controlled Substances), violations of Title 18 U.S.C. § 3147 (Commission of a Crime while on Release), Maryland Criminal Code § 5-701 (Unauthorized Dispensing of a Prescription Medication), Title 18 U.S.C. § 1513 (Retaliating Against a Witness), and Title 18 U.S.C. § 1958 (Murder for Hire) by David ROBINSON and his known and unknown co-conspirators, including, but not limited to:

a. images;
b. videos;
c. records of incoming and outgoing voice communications;
d. records of incoming and outgoing text messages;
e. the content of incoming and outgoing text messages;
f. voicemails;
g. e-mails;
h. voice recordings;
i. contact lists;
j. data from third-party applications (including social media applications like Facebook and Instagram and messaging programs like WhatsApp and Snapchat);
k. location data;
l. browser history;
m. bank records, checks, credit card bills, account information, and other financial records;
n. evidence of user attribution showing who used or owned the Subject Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the term "records" includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

ATTACHMENT "C"

Because of the possibility that the files examined pursuant to this warrant will include information that is beyond the scope of what the United States has demonstrated the existence of probable cause to search for, the search shall be conducted in a manner that will minimize to the greatest extent possible the likelihood that files or other information for which there is not probable cause to search is not viewed.

While this protocol does not prescribe the specific search protocol to be used, it does contain limitations as to what government investigators may view during their search, and the searching investigators shall be obligated to document the search methodology used in the event that there is a subsequent challenge to the search that was conducted, pursuant to the following protocol:

With respect to the search of any digitally/electronically stored information that is seized pursuant to this warrant, and described in Attachment B hereto, the search procedure shall include such reasonably available techniques designed to minimize the chance that the government investigators conducting the search will view information that is beyond the scope for which probable cause exists.

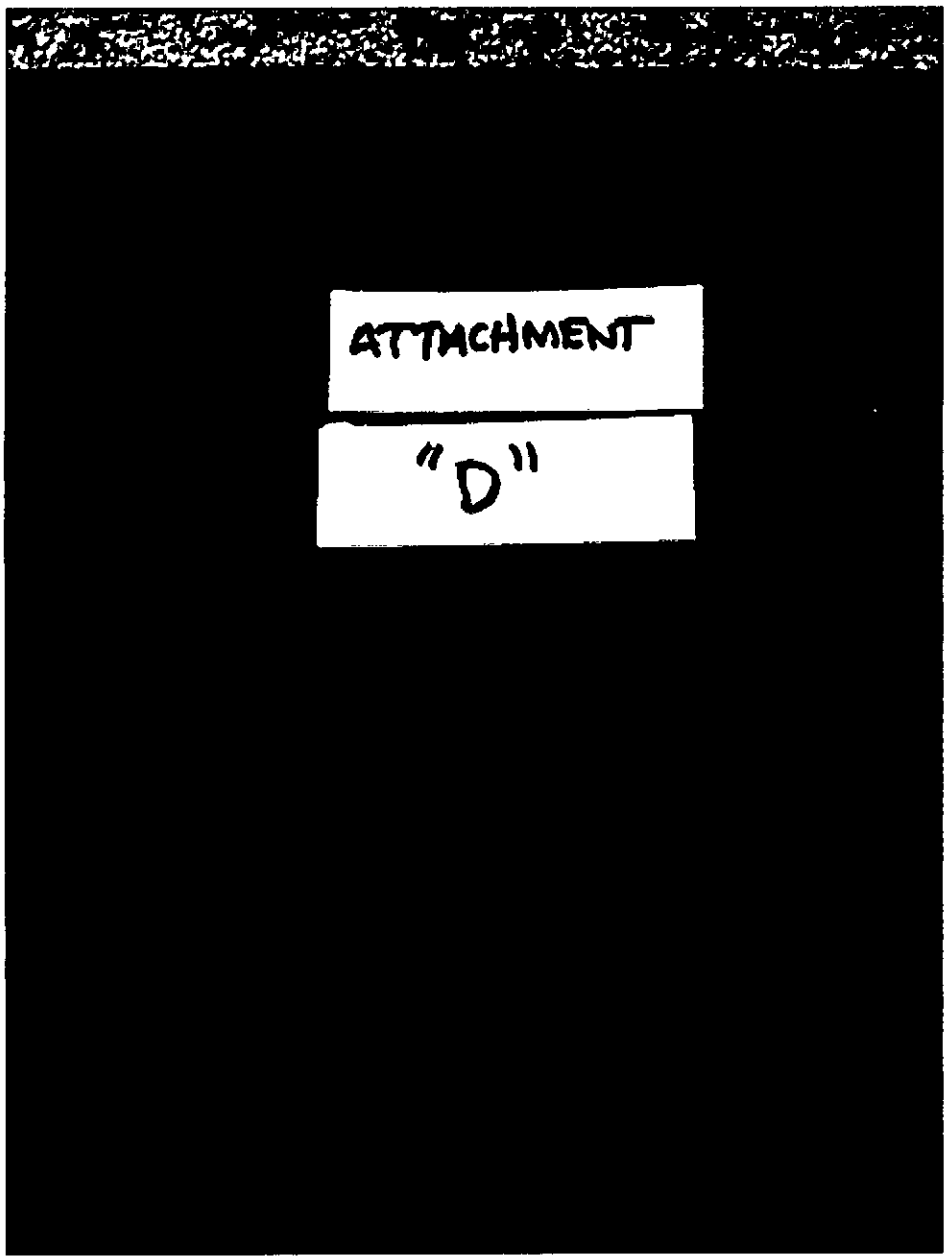
The following list of techniques is a non-exclusive list which illustrates the types of search methodology that may avoid an overbroad search, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein:

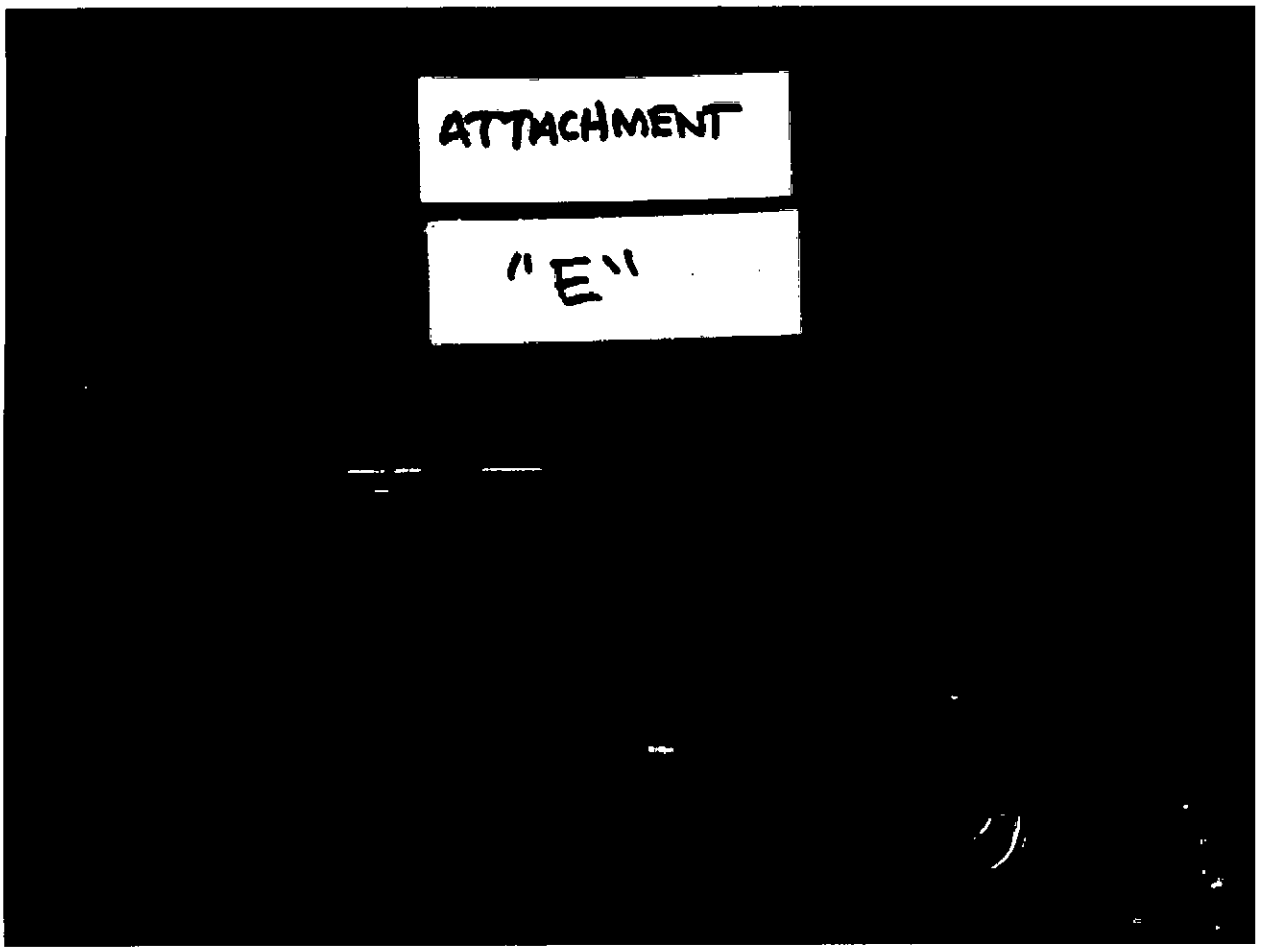
1. Use of computer search methodology to conduct an examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein by specific date ranges, names of individuals, or organizations;

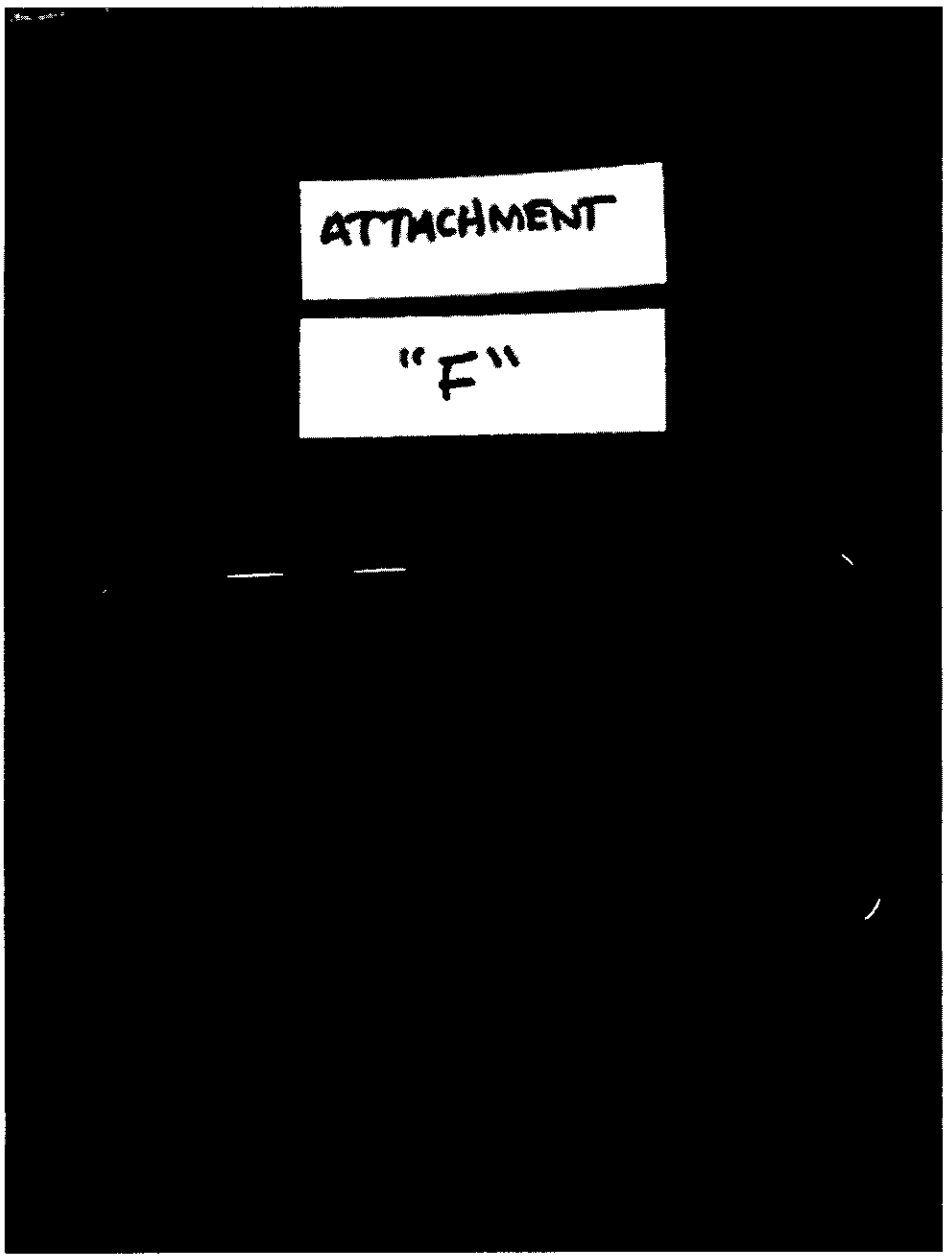
2. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

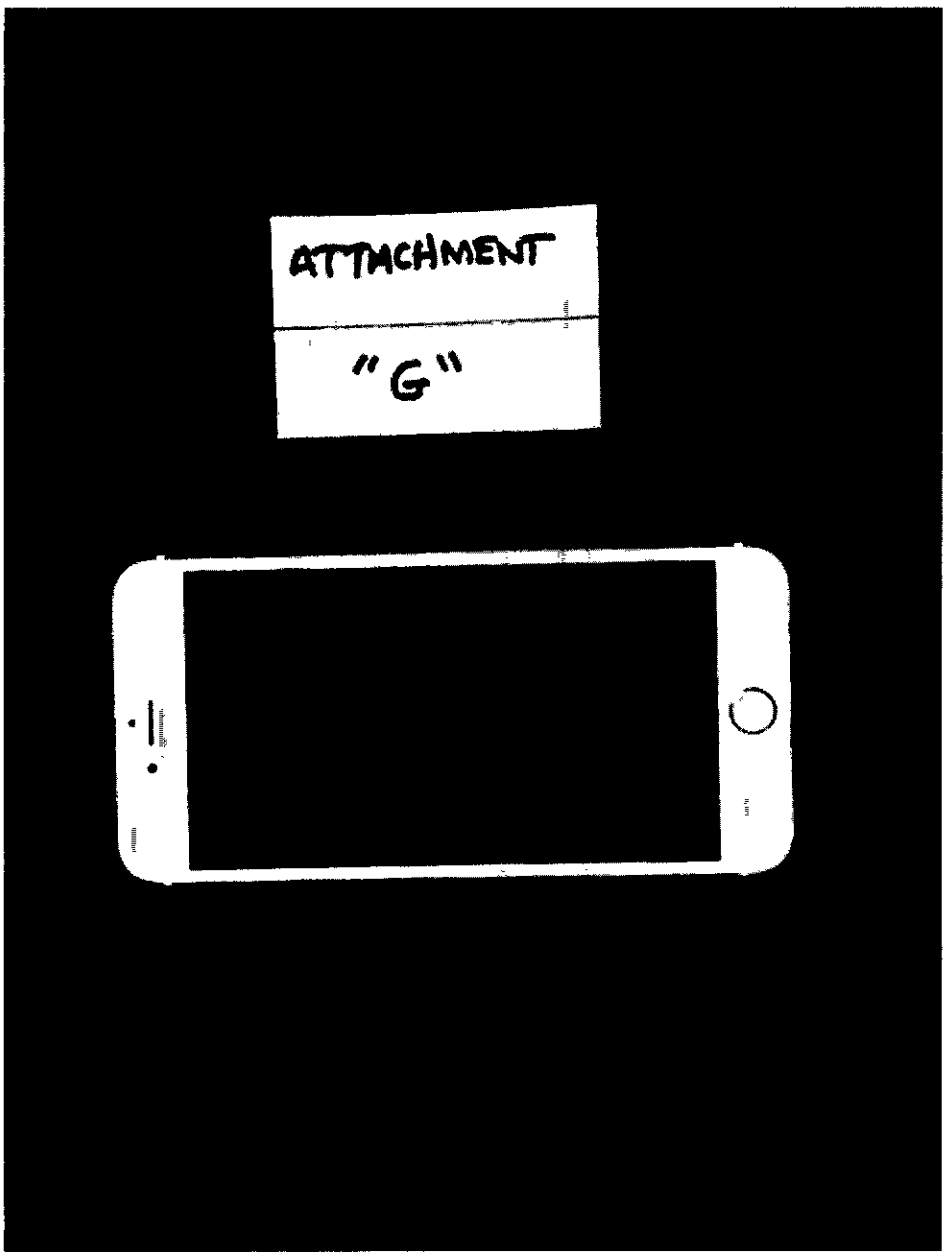
3. Physical examination of the storage device, including digitally surveying various file directories and the individual files they contain, to determine whether they include data falling within the list of items to be seized as set forth herein; and

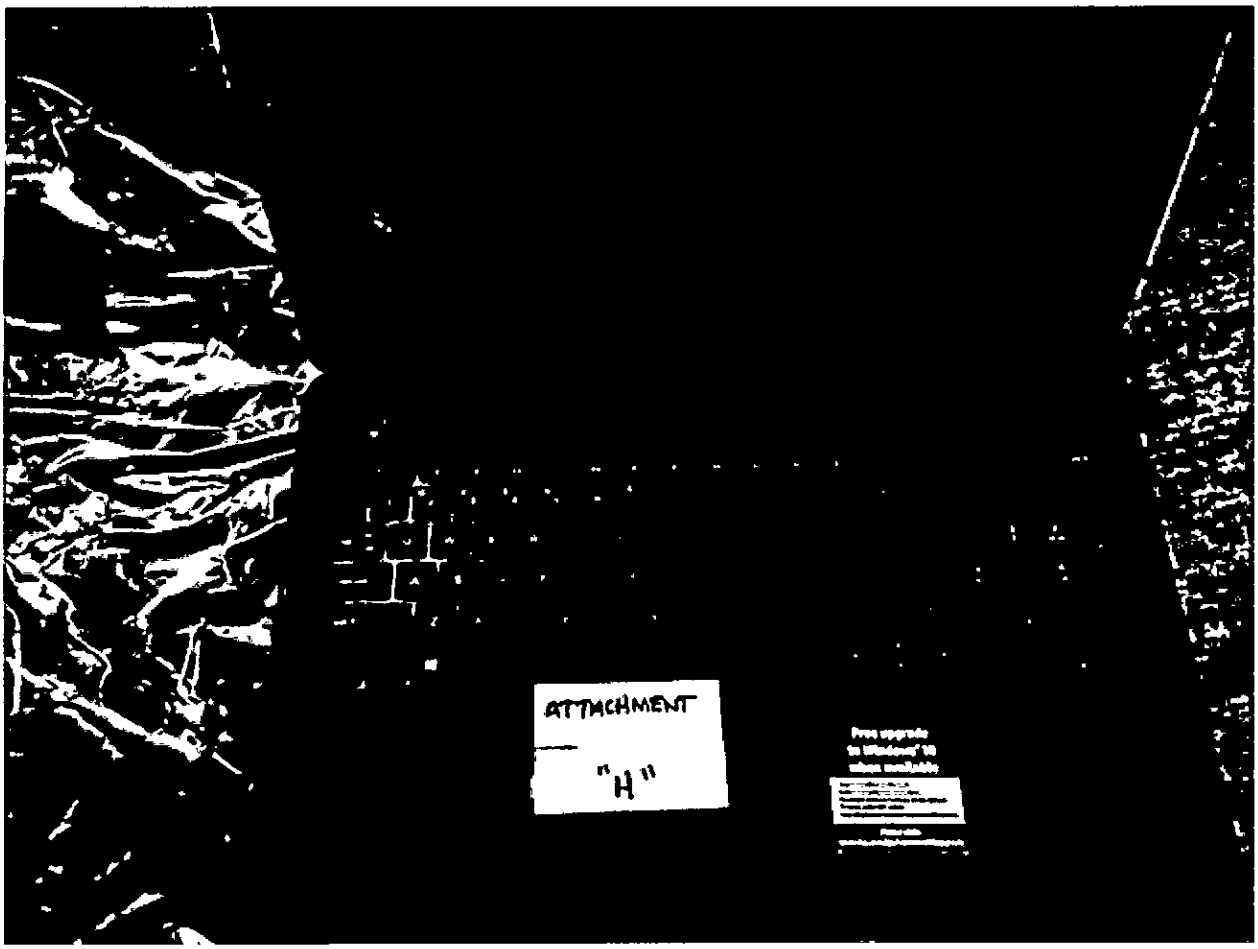
4. Opening or reading portions of files that are identified as a result of conducting digital search inquiries in order to determine their relevance.

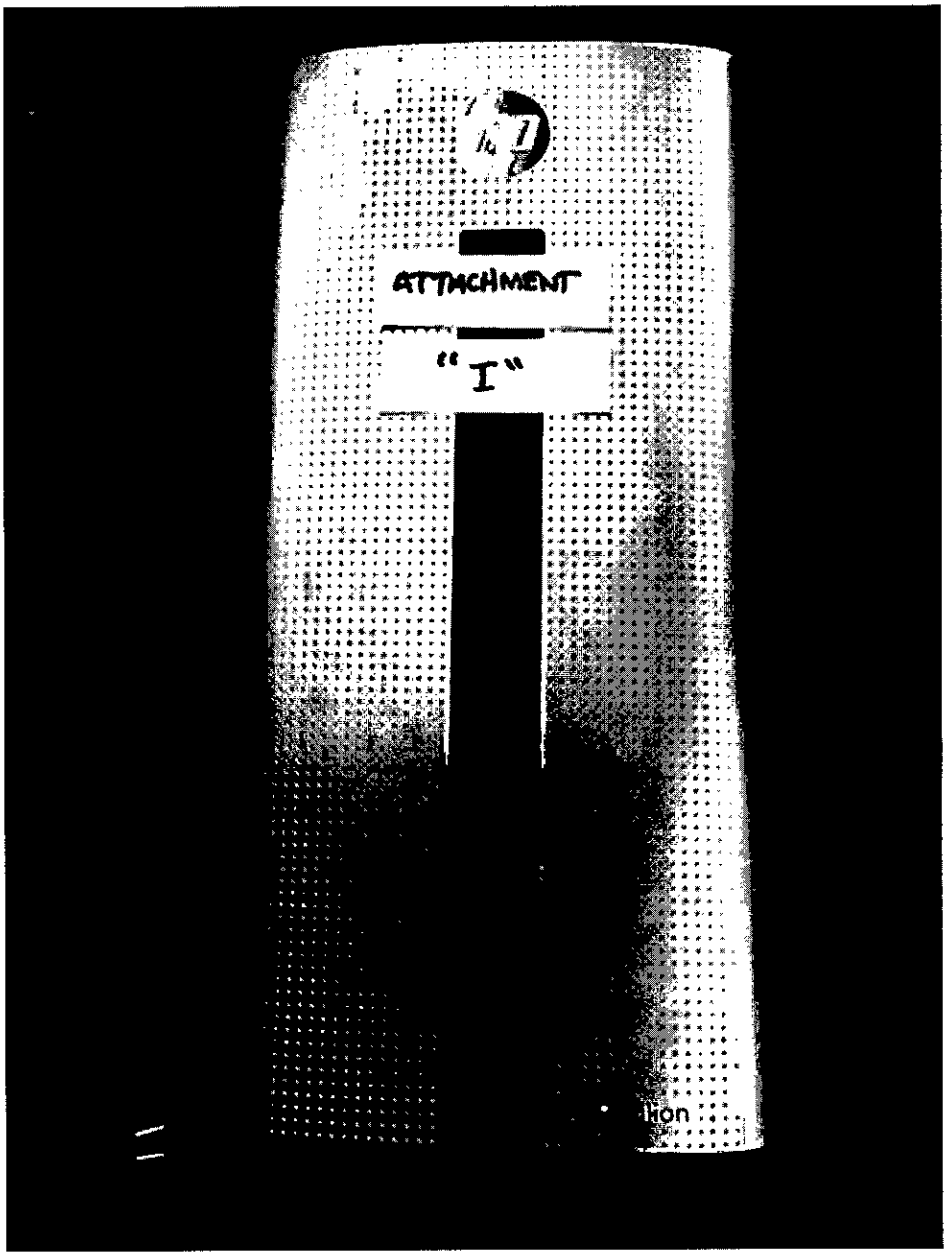

ATTACHMENT
"D"


ATTACHMENT
"E"


ATTACHMENT
"F"


ATTACHMENT
"G"


ATTACHMENT
"H"


ATTACHMENT
"I"

19-833-SAG

EXHIBIT 1